Après l'affaire Snowden, l'anonymat sur internet en question

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE VENDREDI 27 SEPTEMBRE 2013

© Reuters

Les révélations du whistleblower ont mis en lumière une surveillance générale du net mais également une série d'outils permettant d'y retrouver un peu de confidentialité. Même si certains formats populaires, comme HTTPS ou SSL, pourraient eux-mêmes être corrompus...

Révélations après révélations, les documents livrés par Edward Snowden, les moyens déployés par les agences de renseignement, et leurs avancées en matière de cybersurveillance, dépeignent un tableau de plus en plus sombre de l'état de la protection de notre vie privée sur internet. Dans un premier temps, l'ex-employé de la NSA a révélé l'existence d'un système d'espionnage mondial baptisé PRISM déjà particulièrement inquiétant.

© Reuters

Mais jusqu'à présent, beaucoup d'internautes pensaient pouvoir contrecarrer cette surveillance en utilisant divers outils particulièrement populaires. Depuis quelques mois, on a vu fleurir dans les médias généralistes des noms de logiciels et services jusqu'alors plutôt réservés aux spécialistes. *« PGP »*, *« Tor »*, *« Lavabit »* ou encore *« Silent Circle »* sont devenus des acteurs centraux du combat des whitleblowers et de leurs alliés contre les atteintes aux libertés individuelles. Le nombre d'utilisateurs du logiciel de chiffrement PGP, utilisé par Edward Snowden, a par exemple explosé. Selon **le site sks-keyservers.net**, la quantité de *« clefs »* de chiffrement créées quotidiennement a été multipliée par trois ou quatre depuis le mois de juin, passant d'une moyenne de 500 à quelque 1 000 à plus de 2 000 clefs générées. Même son de cloche du côté de Tor, un réseau d'anonymisation qui a vu son nombre d'utilisateurs et son trafic **doubler depuis le mois de juin**.

Au point que, pour certaines catégories comme les journalistes, ne pas les utiliser serait devenu une faute professionnelle. Comme l'a affirmé Edward Snowden **au journaliste du *New York Times* Peter Maas** : *« Dans le sillage des révélations de cette année, il devrait être clair que des communications non chiffrées entre un journaliste et une source sont une imprudence impardonnable. »*

« On se rend compte aujourd'hui, avec PRISM, la surveillance de masse ou avec le modèle économique de géants comme Google ou Facebook, de la fragilité de notre infrastructure de communications », explique Jérémie Zimmermann, porte-parole de l'association de défense des droits des internautes **La Quadrature du net**. *« Tout ce qu'on échange, la plupart du temps, ce sont des cartes postales que tout le monde en chemin peut attraper et lire avant de les laisser continuer. On en vient à se dire que c'est tout l'internet, l'ensemble de nos communications interpersonnelles, qui devrait être chiffré, anonymisé et sécurisé. »*

Malheureusement, au fur et à mesure qu'Edward Snowden continue à diffuser de nouveaux documents, on se rend compte que la situation est encore plus grave et que ces outils eux-mêmes pourraient être corrompus. Certains, comme le spécialiste français de la cryptographie Éric Filiol, vont jusqu'à décrire un mirage monté de toutes pièces par les Américains pour mieux contrôler et surveiller les réseaux. *« La grande capacité des Américains »*, explique-t-il, *« c'est d'imposer des standards qu'ils contrôlent »*. Ainsi, selon cette théorie, les outils d'anonymats ne seraient qu'une création des autorités elles-mêmes, qui

se seraient assuré au passage un accès à toutes les communications chiffrées. Paranoïa ? Pas si sûr si l'on en croit les révélations du ***Guardian*** du vendredi 6 septembre. Selon des nouveaux documents d'Edward Snowden, les services de renseignements américain et britannique auraient en effet réussi, en 2010, à forcer la technologie de chiffrement utilisés par des millions d'internautes.

L'une des premières choses à savoir lorsque l'on veut se protéger sur internet, c'est que l'anonymat total est quasiment impossible à atteindre. *« Quand on parle de sécurité des communications personnelles »*, insiste de son côté Jérémie Zimmermann, *« il faut garder en tête que la sécurité absolue, ça n'existe pas. Il n'y a pas un outil, une baguette ou une formule magique qui va te permettre de sécuriser et d'anonymiser toutes tes communications. » « Il n'y a pas de truc particulier et encore moins d'arme absolue »*, confirme Olivier Laurelli, alias Bluetouff, hacker et co-fondateur du site d'information **Reflets.info**. *« Il y a d'un côté la protection des données, donc le chiffrement, et de l'autre tout ce qui est mesures d'anonymisation. Et à chaque fois, il faut choisir, en fonction du contexte et des besoins, parmi tout un tas de mesures de protection. »*

Un dosage difficile à trouver pour le néophyte. Malgré des efforts notables de vulgarisation, l'installation et l'usage de ces outils, que nous allons détailler par la suite, nécessitent encore souvent quelques compétences techniques, ou l'aide d'un ami… Et il faudra constamment garder à l'esprit qu'un seul système de protection n'est pas totalement fiable. *« Si, par exemple, vous êtes la cible d'une agence de renseignement américaine ou d'une mafia particulièrement puissante »*, prévient Jérémie Zimmermann, *« vous aurez beau installer ce que vous voulez et cliquer sur tous les* "Tor Button" *que vous souhaitez, vous ne serez jamais en sécurité. »*

PGP : l'outil indispensable des mails sécurisés

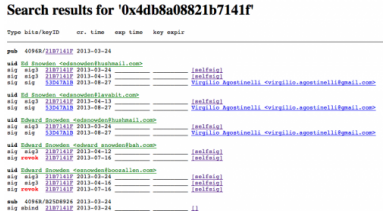
Edward Snowden et son ordinateur © *Twitter*

En matière de chiffrement, les logiciels stars se nomment **PGP, pour *« Pretty Good Privacy »*** (*« Assez bonne confidentialité »*, créé en 1991 par l'Américain Philip Zimmermann et aujourd'hui **détenu par Symantec**, et son équivalent dans le domaine **du logiciel libre, GPG**, pour GNU Privacy Guard. Ces deux outils permettent de chiffrer n'importe quel fichier ainsi que d'assurer la confidentialité et l'authentification des communications.

Concrètement, l'utilisateur se voit attribuer une *« empreinte digitale »* permettant de l'identifier avec certitude, ainsi que deux *« clefs cryptographiques »*, l'une publique et l'autre privée. La première est, comme son nom l'indique, destinée à être diffusée, et l'autre conservée secrète par l'utilisateur. Si quelqu'un veut lui transmettre un contenu, l'envoyeur téléchargera la clef publique avec laquelle il chiffrera le mail ou le fichier en question. Et celui-ci ne pourra être déchiffré qu'avec la clef privée correspondante. L'empreinte digitale permet en outre d'authentifier l'expéditeur, évitant ainsi les usurpations d'adresse.

Pour faciliter les choses, il existe un certain nombre d'annuaires complets permettant de rechercher les clefs publiques de personnes que l'on souhaite contacter. Ceux-ci offrent un certain nombre d'informations, comme les différents mails utilisés par une personne. Voire peut-être un peu trop…

Récemment, en partant de quelques mails chiffrés et en utilisant ces annuaires, **un internaute a réussi mettre au jour** des liens apparents entre plusieurs clefs, échangées entre Edward Snowden et certains de ses contacts. L'ex-employé de la NSA est en effet un utilisateur de PGP, avec différents mails, et certainement plusieurs identités numériques. Des internautes ont par exemple repéré l'omniprésence, dans les contacts chiffrés du whistleblower avec ses proches contacts, d'**un mystérieux***« Michael Vario »*, qui pourrait être un alias pour Edward Snowden ou un autre complice.



Un annuaire de clefs PGP

L'installation du logiciel PGP pourra sembler à beaucoup un peu trop technique. Mais une fois son empreinte et ses clefs créées, il existe bien des logiciels permettant d'implémenter directement le chiffrement dans sa boîte mail habituelle. Il existe également plusieurs services proposant leurs propres solutions de mails sécurisés intégrées. On sait ainsi qu'Edward Snowden utilisait le site Lavabit. Mais celui-ci a **fermé au début du mois d'août** après avoir reçu l'ordre de coopérer avec le gouvernement. Dans la foulée, le site Silent Circle, proposant le même type de services et fondé par l'inventeur du PGP, Phil Zimmermann, avait également mis la clé sous la porte. À noter qu'en France, l'informaticien et pionnier du net Laurent Chemla vient de relancer un ancien projet de mail sécurisé **baptisé***« Caliop »*.

Bien entendu, chiffrer les dossiers stockés sur votre ordinateur et vos échanges de mails ne suffit pas. Il faut également sécuriser votre connexion à internet. Pour cela, il existe déjà une série d'applications dont la plus connue est le module complémentaire ***« HTTPS Everywhere »***, disponible pour les navigateurs Firefox et Chrome. Développé par l'association Electronique Frontier Foundation, ce petit programme permet d'automatiser le protocole *« https »* afin d'assurer, en théorie, l'anonymat des informations transmises à un site.

Pour ceux qui requièrent un peu plus d'anonymat, il sera nécessaire de plonger dans le vaste ensemble que constituent les *« réseaux anonymes »*, encore appelés *« P2P anonymes »*. Derrière cette dénomination un peu floue, se cache une flopée de réseaux développés au sein d'internet avec un protocole spécifique leur permettant d'assurer l'anonymat des données qui y transitent.

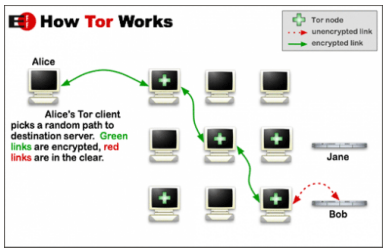
Plusieurs services co-existent, chacun présentant ses avantages et inconvénients en matière de sécurisation et de confort d'utilisation. Particulièrement lent, ***« Freenet »***est par exemple une des solutions les plus sûres pour héberger et publier des documents anonymes. Dans ce réseau, chaque utilisateur héberge, sur son ordinateur, une petite partie du réseau qui se trouve ainsi entièrement décentralisé. Il sera quasiment impossible de faire totalement disparaître une information qui y a été mise en ligne. ***« I2P »*** est lui aussi un réseau décentralisé en général plus rapide que Freenet, ce qui le rend plus adapté à l'utilisation de services tels que le téléchargement, les messageries instantanées ou les mails.

Mais le plus connu, le plus utilisé, et le plus médiatisé, est sans aucun doute le réseau Tor, pour *« The Onion Router »*.

Le phénomène Tor

Tor est en effet l'un des outils privilégiés des hacktivistes, et notamment par Edward Snowden si l'on en croit l'autocollant du *« Tor Project »***collé sur son ordinateur**. Il est notamment utilisé par des ONG ou des plateformes de whistleblowing pour assurer une connexion sécurisée aux lanceurs d'alerte et dissidents politiques. Plus récemment, les Anonymous et le groupe de hackers Telecomix y ont hébergé **un site d'informations et de conseils** à destination des civils syriens ou encore **les données personnelles des leaders de la Syrian Electronic Army**, une pseudo armée de hackers pro-Assad. Tor est enfin utilisé

par **de nombreux services et applications** internet ou mobiles à destination des journalistes amateurs, dissidents ou reporters travaillant en zone de guerre.



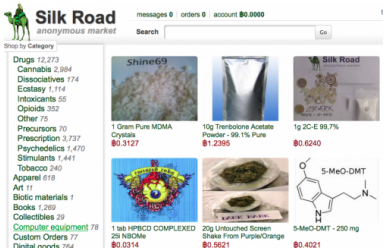
Comment fonctionne Tor © *EFF*

Ce petit programme repose sur toute une série de routeurs organisés en nœuds, ou *« couches »*, hébergés par des volontaires dans le monde entier et au travers desquels les connexions des utilisateurs *« rebondissent »* afin d'être anonymisées. Concrètement, lorsque vous vous connectez à internet via Tor, vos informations sont envoyées à un premier routeur qui les chiffre avant de les envoyer, selon un chemin aléatoire, à un autre, qui les chiffre à son tour… Et ainsi de suite jusqu'au dernier nœud qui déchiffrera la communication pour la délivrer au destinataire final. Intégré à un navigateur internet, Tor permet ainsi de se connecter à internet en déjouant la surveillance de votre fournisseur d'accès ou de toute personne espionnant votre connexion, mais également de visiter n'importe quel site de manière totalement anonyme.

Sur le même principe, Tor permet d'anonymiser des sites internet en masquant les adresses IP de leurs serveurs qui permettraient de les localiser. Dans ce cas, l'utilisateur se connecte au réseau Tor mais, au lien d'en ressortir, accède à des sites aux adresses étranges, souvent une simple suite aléatoire de caractères, se terminant par le suffixe .onion. Il s'agit des fameux *« hidden service »*.

Au sein de ce réseau totalement anonyme, on trouve un peu de tout. Des sites proposant des services, d'emails, de forums de discussion, de partage de fichiers, des sites d'informations parfois extrêmement pointus sur l'informatique, le hacking, et sur le réseau Tor lui-même, des blogs d'informations sur la cybersurveillance et la liberté d'expression…

Anonymat oblige, Tor attire également un nombre difficilement quantifiable de services beaucoup moins légaux. Le plus connus d'entre eux, Silk Road, est même devenu le symbole de ce que les médias ont baptisé le *« darknet »* ou encore *« darkweb »*. En quelques clics, l'utilisateur peut en effet commander quasiment toutes les drogues connues, des mots de passe pour des sites payants, des logiciels de piratage, des cartes de paiement vierges… Quelques autres sites proposent drogues, armes ou données privées, contenus zoophiles et pédophiles, ou divers services difficilement vérifiables, comme ceux d'une agence de tueurs à gages.



Le site Silk Road

Dans la mesure où beaucoup de ces sites ne sont pas référencés, il est difficile de connaître l'étendue exacte de ce *« darknet »* et pas davantage son efficience. Si quelques-uns, comme Silk Road, ont une activité illicite avérée, beaucoup d'autres sont tout bonnement des tentatives d'arnaque, voire des sites vides ou inactifs. De même, si le réseau Tor a bien servi à héberger des serveurs de sites pédophiles, ces derniers ne sont pas, contrairement à une idée propagée par les médias, accessibles en quelques clics. Au bout du compte, en dehors de deux-trois sites connus, ce fameux *« darknet »* peut même sembler bien sage par rapport à l'image qu'on lui colle.

« C'est surtout un grand fantasme », affirme le hacker, et utilisateur de Tor, Koolfy. *« En tout cas, personnellement, je n'ai jamais été confronté à ce genre de choses. C'est sûr que ça existe, mais c'est difficile d'en mesurer l'ampleur car d'éventuels criminels vont chercher à rester cachés et vont utiliser d'autres outils. Tor est un outil pour la liberté d'expression. Or, un criminel n'a pas forcément envie de s'exprimer sur ses crimes. Bien sûr, ça peut lui être utile, mais ça ne sera pas son outil principal. »*

« Le terme “darknet”*, je ne l’ai vu utiliser que dans le milieu de la presse »*, insiste Benjamin Sonntag, informaticien et co-fondateur de La Quadrature du net. *« Je crois qu’il n’existe que dans la tête des journalistes. »« Si tu poses la question à des gens qui ont codé Freenet ou qui ont codé Tor,* “pourquoi avez-vous voulu créer un darknet ?” *»*, poursuit Jérémie Zimmermann, *« ils vont te regarder avec des gros yeux et ils vont te dire* “non, nous on a fait des outils pour sécuriser les communications”. *»*

Même si tout recensement exhaustif est impossible, **une récente étude** menée par des chercheurs de l’université du Luxembourg permet de se faire une petite idée de l’utilisation de ces *« hidden services »*. Sur les 39 824 sites étudiés, les auteurs ont noté une proportion quasi égale entre sites proposant des services illégaux, ou se présentant comme tels, et sites consacrés à la politique ou à l’anonymat. Plus étonnant, et plus inquiétant, les *« hidden services »* les plus visités n’appartiennent à aucune de ces deux catégories mais servent, en réalité, à contrôler des *« botnets »*, des réseaux de programmes informatiques connectés à internet servant, bien souvent, à des attaques informatiques…

Des chercheurs sèment le doute

Sur mediapart.fr, un objet graphique est disponible à cet endroit.

Finalement, plus que de pécher par excès d’anonymat en hébergeant des sites illégaux, le véritable problème de Tor est peut-être, au contraire, de ne pas être encore assez sécurisé. Malgré ce qu’affirment ceux qui vantent, ou dénoncent, son inviolabilité, le réseau est bien loin d’être inattaquable. Ses concepteurs avertissent eux-mêmes, sur **la page de présentation du projet**, que Tor n’est qu’une solution parmi d’autres et qu’elle ne protège pas contre tous les types de surveillances et d’attaques.

Au début du mois d’août, le FBI a ainsi réussi, en utilisant une faille dans une application du navigateur Firefox, à attaquer un hidden-service hébergeant des contenus pédopornographiques dans le cadre d’une enquête ayant conduit à l’arrestation d’un homme en Irlande. Autre sujet d’inquiétude, Tor a vu son trafic doubler depuis le mois de mai dernier. Si ces bons chiffres peuvent tout simplement être la conséquence d'un *« effet de mode »* ou une prise de conscience provoquée par l’affaire Snowden, certains comme Roger Dingledine, l’un des créateurs de Tor, **suspectent une potentielle attaque** informatique de botnets.

Ces dernières années, plusieurs chercheurs ont remis en cause la fiabilité du réseau, affirmant que l’identification d’un utilisateur ne serait qu’une question de temps pour un attaquant disposant des moyens techniques suffisants. Parmi eux, Éric Filiol, ce spécialiste français de la sécurité informatique et de la cryptographie et directeur du laboratoire de virologie et de cryptographieinformatique de l'ESIEA. Avec ses élèves, il a réussi en 2011 à mettre au point une attaque qui leur a permis d’extraire les informations contenues dans des nœuds du réseau Tor. La publication des travaux de l’équipe d’Éric Filiol, présentés à Berlin durant la célèbre convention de hackers ***« Chaos Communication Congress » (CCC)***, a suscité des réactions parfois très vives.

Sur mediapart.fr, une vidéo est disponible à cet endroit.

« J’ai été extrêmement choqué par la manière dont les gens réagissaient, car 90 % de ceux qui nous critiquaient n’avaient jamais mis le nez dans le code source de Tor ni lus nos travaux », raconte aujourd’hui le chercheur français. Sans rentrer dans les détails techniques, certains hackers, comme Koolfy qui a consacré **plusieurs articles au sujet**, lui reprochent notamment d’avoir utilisé une attaque bien connue contre le réseau Tor pour extraire des informations. En résumé, la démonstration d’Éric Filiol n’apporterait rien de neuf et ne remettrait pas en cause l’intégrité même du réseau.

Mais l’intéressé va beaucoup plus loin. Il affirme aujourd’hui que sa démonstration n’était qu’un exemple du manque de fiabilité de Tor et s’inscrivait dans un cadre beaucoup plus large, et beaucoup plus inquiétant. *« Le projet Tor est en fait né à l’école post-navale de Monterey »*, explique-t-il. *« Il s’agissait d’un projet de très haut niveau mais fait par des militaires. Ensuite, Tor est devenu une fondation qui a commencé à diffuser le logiciel. Or, qui est son*

président ? Roger Dingledine, un ancien de la NSA. C'est d'ailleurs quelque chose qu'il ne cache pas : ***c'est dans son CV****. »*

Éric Filiol remet également en cause le caractère aléatoire du réseau de nœuds à la base de Tor. *« Un utilisateur de Tor va obligatoirement se connecter en passant par cinq points d'entrée, tous situés sur le territoire américain, et donc soumis au Patriot Act. Et ces cinq points sont gérés par qui ? Trois par Jacob Appelbaum* (NDLR : un hacker assurant les fonctions de porte-parole de Tor)*, un par Dingledine, un par Mike Perry* (NDLR : un développeur participant au projet Tor)*. C'est facile, y a les adresses IP ! »* Les soupçons d'Éric Filiol ont récemment été **confortés par une nouvelle étude**, américaine cette fois, remettant en cause la protection de l'anonymat sur le réseau et devant être présentée au prochain CCC, au mois de décembre prochain. Et on sait par ailleurs, grâce au rapport financier de la fondation Tor, que le premier mécène du projet était, en 2012, **le ministère de la défense américain** via une bourse de 876 000 dollars accordée par l'Institut de recherche de Stanford.

En somme, à en croire cette théorie, Tor, le réseau anonyme le plus populaire, serait une autre création de l'armée américaine. Dans quel but ? *« L'idéal, quand l'on veut surveiller quelqu'un, c'est de lui laisser croire qu'il est protégé »*, répond Éric Filiol. *« Pour mieux le contrôler... Les gens qui ont quelque chose à cacher, que font-ils ? Ils communiquent en chiffré »*, explique-t-il. « *Imaginez une foule où tout le monde parle français. Et au milieu des personnes qui se mettent à parler une autre langue. Vous allez immédiatement les identifier. »* Ensuite, ne reste plus qu'à intercepter la communication… et à la traduire.

« On verse dans la parano absolue »

Mais même sur ce point, Éric Filiol affirme que les dés sont pipés, mettant à bas les bases mêmes du chiffrement des données utilisé par la plupart des outils d'anonymat. *« Ces réseaux sont tous sécurisés par de la cryptographie. Or, aujourd'hui, celle-ci repose sur un seul et même standard : l'AES. Et ce standard est bien entendu américain. En 2001, une agence du département du commerce, le NIST (National Institute of Standard and Technology) a lancé un concours. Et quel était l'organisme certificateur ? La NSA… Comme je l'expliquais à l'époque :* "Vous croyez qu'en pleine montée du terrorisme et de l'altermondialisme, ils vont distribuer à tout le monde un algorithme inviolable ?" »

« À partir du moment où Tor, ou n'importe qui d'autre, prend de la crypto d'obédience américaine, c'est fini, ils sont attrapés. Mais bon, si ça ne choque personne… »« La vraie question, c'est l'idée d'un réseau d'anonymisation qui ne soit pas sous contrôle », conclut Éric Filiol. *« Or, c'est un rêve, un mythe. Aucun pays ne laisserait faire ça. Tout est sous-contrôle, et depuis le début. »*

La NSA © Reuters

Cette thèse a de quoi faire bondir bon nombre d'hacktivistes. *« Oui, la NSA a participé à la relecture du standard AES, mais comme tout le monde »*, réagit ainsi Koolfy. *« S'il y avait la moindre anomalie dans le code, il y aurait forcément quelqu'un pour s'en rendre compte. C'est une valeur sûre. »* Concernant Tor, le hacker confirme qu'il s'agit *« d'un outil qui sert aussi à la NSA et ce sont bien les Américains qui en ont exprimé le besoin. Mais c'est un outil open source, c'est-à-dire que le code source est totalement public. N'importe qui ayant la moindre suspicion sur les intentions des auteurs peut le vérifier. »*

« Oui, en un sens, il suffit qu'un bout de routage de Tor passe par les États-Unis pour qu'il soit soumis au Patriot Act », estime de son côté Bluetouff. *« Mais je ne pense pas me tromper quand je dis que la NSA est bien emmerdée lorsqu'elle tombe sur du Tor. Pour l'instant, ils ne savent pas quoi en foutre. Donc, qu'est-ce qu'ils font ? S'ils peuvent stocker, ils stockent. »* De même, concernant le chiffrement, il existerait *« des niveaux de chiffrement sur lesquels on pourrait faire tourner des grappes d'ordinateurs énormes pendant*

des dizaines d'années sans parvenir à casser le mot de passe. » « Éric Filiol est loin d'être idiot. Il sait de quoi il parle. Mais, là, on verse dans la parano absolue. »

Et au-delà des débats d'experts, et au risque de sombrer effectivement dans la paranoïa, tous se rejoignent sur un point : ni Tor ni aucun autre logiciel ne peut suffire à assurer totalement votre anonymat. *« Le seul fait d'utiliser ce type de technologies est en soit une manière de se faire repérer »*, estime ainsi Jérémie Zimmermann. *« Par exemple, si vous vous connectez du jour au lendemain à Tor depuis un réseau d'entreprise, il y aura quelqu'un du service informatique qui va le repérer et vous mettre sous surveillance. En Chine, utiliser Tor, c'est porter un gros gyrophare rouge et une pancarte disant* "je n'aime pas ce régime". *Et une fois que l'on est repéré, l'identification n'est qu'une question de temps. »« On peut voir votre ordinateur comme une maison. Et votre connexion à internet, c'est la porte »*, explique Éric Filiol. *« Avec un outil comme Tor, vous allez peut-être blinder la porte, mais si votre maison est en carton, ou si vous avez laissé vos clefs sous le paillasson, cela ne sert pas à grand-chose… » « Il y a mille façons d'obtenir des informations »*, confirme Jérémie Zimmermann. *« On peut s'introduire dans ton ordinateur et obtenir ce que tu tapes au moment où tu le tapes avant même que tu l'envoies sur le réseau Tor, voir ce que tu vois sur ton écran, etc.»*

Au bout du compte, la sécurité informatique ne serait donc qu'une illusion ? *« Oui et non »*, tempère Benjamin Sonntag. *« Les milieux militaires américains n'auront aucun problème à accéder à n'importe quel ordinateur. Mais il faut être une de leurs cibles car cela nécessite des techniques qu'ils ne peuvent pas appliquer en masse. »* En résumé, les outils comme Tor ou GPG sont effectivement efficaces contre la surveillance *« quotidienne »*, c'est-à-dire celle des publicitaires, des sites que vous visitez, voire celle de certains services répressifs de l'État chargés, par exemple, de lutter contre le téléchargement. Mais si ce que vous avez à cacher intéresse une quelconque agence de renseignement, vous ne trouverez aucun lieu sûr sur le réseau.

Dans ce cas, il ne vous restera plus que les *« bonnes vieilles méthodes »*. *« Si j'avais un document extrêmement sensible à diffuser »*, affirme Bluetouff, *« il n'y a pas un seul échange qui passerait par internet. Ça ne passerait par aucune machine »*. Au mois de juillet dernier, le FSO, un service russe issu de l'ex-KGB, a ainsi décidé **de revenir à la machine à écrire**. *« Du point de vue de la sécurité, tout type de télécommunication électronique est vulnérable. On peut capter n'importe quelle information depuis un ordinateur »*, déclarait alors au journal *Izvestia* le député et ex-directeur du FSB (ex-KGB) Nikolaï Kovalev. *« Le moyen le plus primitif est à privilégier : la main humaine ou la machine à écrire. »*

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.
Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.